AMENDMENTS TO THE CLAIMS

Please amend the claims by replacing the original claims with the following listing of claims.

LISTING OF THE CLAIMS:

1. (Currently amended) A method for securing, maintaining, monitoring and controlling computer networks and clients located therein, comprising: providing a hash code table of a client <u>said hash code table being provided for storing a plurality of files</u>; providing a client state code of a client; comparing said client state code to said hash code table, and generating an alert mechanism when a deviation threshold is reached based on a deviation between said hash code table values for said client and said client state code.

2. (Original) A method as in claim 1 wherein the step of providing a hash code table of a network device further comprises providing a secure hash code table.

3. (Original) A method as in claim 2 wherein the step of providing a secure hash code table further comprises generating a secure hash code table.

4. (Original) A method as in claim 3 wherein the step of generating a secure hash code table further comprises generating a secure hash code table using at least one compiled client hash value.

5. (Previously presented) A method as in claim 3 wherein the step of generating a secure hash code table further comprises generating a secure hash code table using at least one compiled client hash value, wherein said compiled client hash value is generated by: providing a secure system state data file; grouping said secure system data file into one or more groups; and, extracting the modal hash value from any of said groups.

6. (Original) A method as in claim 3 wherein the step of generating a secure hash code table further comprises generating a secure hash code table using at least one exemplary system.

7. (Original) A method as in claim 3 wherein the step of generating a secure hash code table further comprises generating a secure hash code table using at least one baseline secure value.

8. (Original) A method as in claim 1 further comprising the step of reporting the results of said comparison.

9. (Original) A method as in claim 1 further comprising the step of logging the results of

said comparison.

10. (Original) A method as in claim 1 further comprising the step of securing a client in

lock down mode.

11. (Original) A method as in claim 1 further comprising the step of initiating a client

status mechanism.

12. (Original) A method as in claim 1 further comprising the step of initiating an Auto

Restore component.

13. (Original) A method as in claim 1 wherein the step of providing a client state code

further comprises generating a client state code.

14. (Original) A method as in claim 3 wherein the step of generating a client state code

further comprises generating a client state code using at least one compiled client hash

value.

15. (Original) The hash code table generated by any of the methods of claims 4 through

7.

16. (Original) An article for securing, maintaining, monitoring and controlling computer

networks and clients located therein, comprising a client state code.

17. (Original) An article for securing, maintaining, monitoring and controlling computer

networks and clients located therein, comprising a hash code table.

18. (Currently amended) An apparatus for securing, maintaining, monitoring and

controlling computer networks and clients located therein, comprising: means for

providing a hash code table of a client said hash code table being provided for storing a

plurality of files; means for providing a client state code of a client; and, means for

comparing said client state code to said hash code table; and means for generating an

alert when a deviation threshold is reached based on a deviation between said hash code

table values for said client and said client state code.

19. (Currently amended) An apparatus for securing, maintaining, monitoring and

controlling computer networks and clients located therein, comprising: means for

providing a hash code table of a client said hash code table being provided for storing a

plurality of files; means for providing a client state code of a client; and, means for

comparing said client state code to said hash code table, wherein said hash code table is operable for one or more client platforms.

20. (Original) An apparatus as in claim 19 further comprising means for generating a secure hash code table.

21. (Original) An apparatus as in claim 19 further comprising means for reporting the results of said comparison.

22. (Original) An apparatus as in claim 19 further comprising means for logging the results of said comparison.

23. (Original) An apparatus as in claim 19 further comprising a client status mechanism means.

24. (Original) An apparatus as in claim 19 further comprising an Auto Restore component means.

25.   (Previously presented) A method for securing, maintaining, monitoring and controlling computer networks and clients located therein, comprising: providing a hash code table of a client; providing a client state code of a client; comparing said client state

code to said hash code table, wherein said hash code table is operable for one or more

client platforms.

26.   (Previously presented)   The method of claim 25, wherein providing a hash

code table includes gathering baseline values to define modal values and generating said

hash code table using said defined modal values, wherein each of said clients uses the

same or different operating platform as another of said client, and wherein regardless of

the operating platform used by a said client, said client state code is compared to said

generated hash code table.

27.   (Previously presented) The method of claim 25, wherein providing a hash code

table further includes transmitting a secure system state data file from a said client to a

server, and constructing said hash code table from network clients based on one or more

compiled client hash values, the method including grouping secure system state data files

into client groups.